DOI: 10.26314/GARR-Conf17-proceedings-07

# Analisi, valutazione del rischio e sicurezza informatica di dati e informazioni dei dispositivi medici connessi alle reti IT-medicali

Catello Chierchia[1], Enrico Guerra[2], Martina Balloccu[2], Lorenzo Monasta[3], Francesca Deluca[1], Michele Bava[1,2]

[1]Ufficio Sistema Informativo – SC Ingegneria Clinica, Informatica e Approvvigionamenti – IRCCS Burlo Garofolo di Trieste, [2]DIA – Università degli Studi di Trieste, [3]SSD Epidemiologia e Statistica – IRCCS Burlo Garofolo di Trieste

**Abstract.** Questo lavoro ha come scopo la realizzazione di un modello per l'analisi e la gestione del rischio dei dispositivi medici (DM) collegati a una rete IT-medicale. Il modello determina un Indice di Valutazione del Rischio (IVR) che è funzione di alcuni fattori di rischio preventivamente selezionati, calcolando i relativi pesi ottenuti da due modelli statistici: la regressione lineare e il modello logistico.
I fattori di rischio si concentrano principalmente sulla parte informatica che negli ultimi anni sta ricoprendo un ruolo fondamentale nell'ambito della sanità, dove occorrono misure adeguate di sicurezza per proteggere reti ospedaliere, sistemi clinici, dati e informazioni.

**Keywords.** Rete IT-Medicale, Sicurezza informatica, Analisi del rischio, Dispositivi Medici, Metodi statistici

## Introduzione

In un mondo che si avvia verso la completa informatizzazione e digitalizzazione di dati, informazioni e conoscenza, anche il settore ospedaliero e il mondo sanitario in generale si trovano ad affrontare nuove opportunità e sfide che hanno a che fare con la gestione dei dati e la sicurezza informatica. Nella società attuale infatti possiamo considerare la protezione dei dati e le informazioni che essi generano (*data and system security*), come "il nuovo petrolio" (Simi 2016), cambiando e innovando il modo di produrre ricchezza. La mancanza d'idonei strumenti di protezione di una rete dati ospedaliera quindi può portare non solo al danneggiamento del dispositivo che ha generato le informazioni, ma anche rendere la rete stessa facile preda di *hackers* malintenzionati, che realizzano gran parte del loro fatturato con la sottrazione e la violazione di dati di aziende impreparate ad affrontare efficacemente la minaccia (CINI 2017).

È quindi fondamentale, e auspicabile, che gli enti si tutelino con misure di sicurezza adeguate per proteggere capitale, tecnologia e conoscenza, in particolar modo i sistemi e i servizi che trattano dati sensibili, attraverso investimenti sulla messa in sicurezza della rete informatica (CLUSIT 2017). Lo scopo è di ottenere un elevato grado di protezione da attacchi esterni e garantire così la continuità operativa della struttura, ma non basta: è necessario infatti che questo grado di protezione sia periodicamente verificato attraverso



Conferenza GARR 2017 - The data way to Science - Selected Papers
Venezia, 15-17 novembre 2017 - ISBN: 978-88-905077-7-9 

un'analisi del rischio che produca parametri oggettivi per la valutazione di tutti i sistemi, servizi e le apparecchiature collegate alla rete IT-medicale (Cacciari et al. 2015).

## 1. Metodo

Nel progetto proposto, partendo da quanto acquisito in ambito legislativo (D.Lgs. 196/03, nuovo Regolamento Privacy 679/2016), e normativo (ISO 27001, ISO 80001 e ISO 30001) si attribuisce, a ogni apparecchiatura o dispositivo medico (DM) collegato a una rete ospedaliera, un indice, l'Indice di Valutazione del Rischio (IVR), che valuti il relativo livello di sicurezza nelle condizioni d'uso tipiche. L'IVR è ottenuto attraverso l'implementazione di metodi statistici e una stima dei pesi oggettiva che renda il modello ripetibile e quindi convalidabile.

L'IVR è distribuito in un range da 1 (basso rischio) a 10 (alto rischio) e suddiviso in macrocategorie che tengano conto sia delle tematiche tipiche dell'ingegneria clinica (la documentazione e la manutenzione delle apparecchiature, i rischi collegati al paziente) sia di aspetti ICT solitamente trascurati nell'analisi del rischio delle tecnologie biomediche. Attraverso l'assegnazione di una serie di regressori è realizzata la formula per il calcolo dell'IVR relativo al rischio rilevabile sulla singola apparecchiatura nelle condizioni di esercizio.

In particolare per la parte relativa alla sicurezza informatica si è scelto di considerare come regressori la presenza/assenza di credenziali di accesso per accedere al sistema, se è presente ed è aggiornato l'antivirus, se è stato effettuato il backup dei dati, se è avvenuta perdita dei dati, se è attivo il firewall, se il dispositivo è sotto gruppo di continuità e se risulta positivo ai test di vulnerabilità; tutti argomenti che riguardano la privacy, l'information security e la cybersecurity (Bava et al. 2009).

Per ricavare i pesi di ciascuna categoria, nel nostro studio sono stati utilizzati due modelli allo scopo di confrontarne i risultati: la regressione lineare multipla e il modello logi-

| DOCUMENTAZIONE E MANUTENZIONE | | | | |
|---|---|---|---|---|
| **X1 Documentazione completa** | **X2 Controlli e verifiche effettuati periodicamente** | **X3 Disponibilità ditta** | **X4 Costo di manutenzione** | **X5 Disponibilità muletti** |
| Si=0 | Si=0 | Si=0 | Sotto contratto=0 | Si=0 |
| No=1 | No=1 | No=1 | Nessun contratto=1 | No=1 |

| RISCHIO PER IL PAZIENTE | | | |
|---|---|---|---|
| **Y1 Funzione apparecchiatura** | **Y2 Conseguenze per il paziente** | **Y3 Età del dispositivo** | **Y4 Frequenza d'utilizzo** |
| Altro=2 | Nessun rischio =1 | Minore di 8 anni=0 | Annuale=1 |
| Analisi=3 | Terapia inappropriata=2 | Maggiore di 8 anni=1 | Mensile=2 |
| Diagnostica=4 | Danno=3 | | Settimanale=3 |
| Terapeutica=5 | Morte=4 | | Giornalireo=4 |

| SICUREZZA INFORMATICA | | | | | | |
|---|---|---|---|---|---|---|
| **Z1 Credenziali di accesso al sistema** | **Z2 Antivirus** | **Z3 Backup** | **Z4 Perdita dei dati** | **Z5 Test di vulnerabilità** | **Z6 Firewall** | **Z7 UPS** |
| Si=0 | Installato e aggiornato=0 | Effettuato=0 | No=0 | Negativo=0 | Attivo=0 | Si=0 |
| No=1 | Installato e non aggiornato=1 | Non effettuato=1 | Si=1 | Positivo=1 | Non attivo=1 | No=1 |
| | Non presente=2 | | | | | |

Figura 1
Fattori di rischio relativi alla documentazione, rischio paziente e IT security

stico. Nel primo caso si studia la dipendenza di una variabile quantitativa Y dall'insieme dei regressori $X_1,\ldots,X_m$, $Y = f(X_1, \ldots, X_m) + \varepsilon = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_m X_m + \varepsilon$ attraverso un modello lineare (Montanari 2015), e una tripartizione del livello di rischio in alto, medio e basso; nel secondo caso invece il modello di regressione è applicato nei casi in cui la variabile dipendente Y può assumere esclusivamente valori dicotomici, in questo caso alto e medio/basso rischio $Y=\text{logit}(p) = \ln\left(\frac{p}{1-p}\right)$.

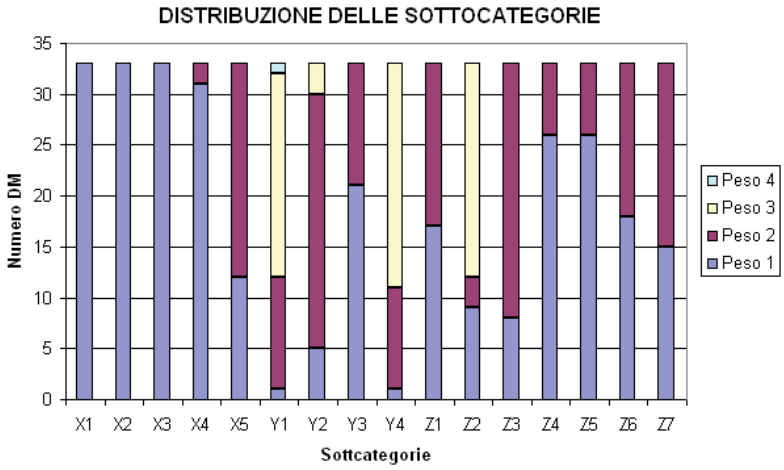



Figura 2
Distribuzione dei DM rispetto le varie sottocategorie/fattori di rischio

## 2. Risultati

I risultati finora ottenuti evidenziano che entrambi i modelli possono essere presi in considerazione ed essere valutati per la stima dei pesi per le singole categorie e quindi trovare l'IVR dell'apparecchiatura; il modello logistico (procedura Firth) però riesce a simulare me-

| MODELLO LOGISTICO PROCEDURA FIRTH | | | |
|---|---|---|---|
| Predizione Lineare | Medio/Basso Rischio | Alto Rischio | Totale |
| -10,51835 | 3 | 0 | 3 |
| -5,56893 | 1 | 0 | 1 |
| -4,652917 | 1 | 0 | 1 |
| -4,243236 | 1 | 0 | 1 |
| -2,740673 | 2 | 0 | 2 |
| -2,619888 | 5 | 0 | 5 |
| -2,505077 | 2 | 0 | 2 |
| -1,294194 | 1 | 0 | 1 |
| -1,149973 | 1 | 0 | 1 |
| -1,002514 | 1 | 0 | 1 |
| -0,5046952 | 2 | 1 | 3 |
| 0,2083686 | 2 | 3 | 5 |
| 1,118652 | 0 | 1 | 1 |
| 1,200816 | 0 | 1 | 1 |
| 2,411699 | 0 | 2 | 2 |
| 3,914261 | 0 | 1 | 1 |
| 3,946909 | 0 | 1 | 1 |
| 6,863303 | 0 | 1 | 1 |
| **Totale** | **22** | **11** | **33** |

Figura 3
Valore di predizione lineare con procedura Firth e cut-off

glio l'andamento desiderato con una sensibilità del 100% e una specificità dell'82%, identificando tutti i dispositivi ad alto rischio, mentre per il medio/basso rischio non individua quattro macchine, ponendole a un livello di allerta superiore al necessario.

## 3. Conclusioni

Avendo un modello ripetibile e convalidabile la prospettiva futura è di impiegarlo nelle strutture ospedaliere per fornire una valutazione del rischio realistica e affidabile, con una formula predittiva che permetta l'intervento tempestivo sul DM e sulla rete dati, riducendo così i possibili rischi legati ad attacchi informatici o relativi allo stato delle apparecchiature. Non solo: l'espansione del suo utilizzo a livello territoriale permetterebbe di centralizzare l'archiviazione dei dati relativi ai DM delle strutture ospedaliere di tutta una regione.

L'aggregazione di una grande quantità di questi dati consentirebbe di applicare il modello descritto al dominio dei big data e ottenere così sia risultati dell'IVR sempre più attendibili, ma anche un sensibile miglioramento nell'attività decisionale. Attraverso lo studio di una tale mole di dati si potrebbero analizzare variazioni dell'IVR e trovare i trend che permettano di prevenire i guasti, garantendo un ciclo di vita più lungo delle macchine e/o inviare un alert alle ASL interessate prima che la criticità diventi troppo rilevante.
Gli stessi big data potrebbero produrre differenti IVR relativi a strutture analoghe e questo essere sintomo di una non adeguata manutenzione e controllo delle apparecchiature stesse.

L'utilizzo di reti neurali o altri sistemi d'intelligenza artificiale o machine learning inoltre, permetteranno di valorizzare ulteriormente la bontà del modello, con un supporto immediato e ancora più efficace alle decisioni in fase di analisi e valutazione del rischio sia locale che globale.

## Riferimenti bibliografici

Bava M.et al. (Indore, India 23-25 July 2009), "Information Security Risk Assesment in Healthcare: the experience of an Italian Pediatric Hospital", CICSYN 2009, pp. 321-326, IEEE Computer Society

Cacciari D., Zotti D., Sossa E., Bava M. (2015), "Infrastructure Security in Pediatric Hospital: Architectural Evolution, Virtualization and Network Management Systems", Special Issue in Advances in Networks- Secure Network Communications, volume 3, Issue 3-1, pp 23-26, Science Publishing Group 2015

CINI Laboratorio Nazionale di Cybersecurity (2017), "Italian Cybersecurity Report", pag. 3

CLUSIT – Associazione italiana per la sicurezza informatica (2017), "Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia"

Montanari A (2015) "La regressione lineare multipla", pag. 1 http://www2.stat.unibo.it/montanari/Didattica/dispensa2.pdf

Simi L. (2016), "I dati sono il nuovo petrolio"

http://www.pagina99.it/2017/03/16/industria-dei-dati-italia-nuovo-petrolio

## Autori

**Catello Chierchia** - catello.chierchia@burlo.trieste.it

Laureato in Ingegneria Clinica presso l'Università di Trieste, da marzo 2017 è ricercatore presso l'IRCCS Burlo Garofalo per la sicurezza informatica dei dispositivi medici in una rete IT-medicale.

**Enrico Guerra** - enricoguerra@live.com

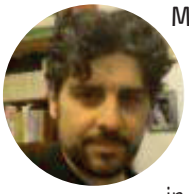
Studente di Ingegneria Clinica presso l'Università di Trieste dove ha coltivato l'interesse per l'informatica sanitaria, sta conducendo la tesi sull'implementazione di un sistema di supporto alla decisione clinica utilizzando IBM Watson.

**Martina Balloccu** - martina.balloccu@gmail.com

Laureata in Ingegneria Clinica presso l'Università di Trieste ha conseguito precedentemente la laurea triennare in Ingegneria Biomedica presso l'Università degli Studi di Cagliari.

**Francesca Deluca** - francesca.deluca@burlo.trieste.it

Laureata in ingegneria clinica presso l'Università di Trieste, dal 2016 è impiegata presso l'IRCCS Burlo Garofolo di Trieste dove si occupa di sistemi informativi sanitari all'interno della S.C. Ingegneria Clinica, Informatica e Approvvigionamenti.



**Michele Bava** - michele.bava@burlo.trieste.it

Laureato in Ingegneria Elettronica, Specialista in Ingegneria Clinica e Informatica Medica, PhD in Ingegneria dell'Informazione lavora dal 2003 presso l'Ufficio Sistema Informativo dell'IRCCS Burlo Garofolo di Trieste e dal 2009 in qualità di Amministratore di Sistema. Negli anni titolare di diversi progetti di ricerca svolge attualmente ricerche nel campo dell'ICT in Sanità, della Telemedicina e della Sicurezza Informatica.